INFORMATION SECURITY ANALYST IV

GRADE 40
FLSA Status: Exempt

GENERAL DEFINITION OF WORK:

Under general supervision this senior level position is responsible for planning and implementing security measures to protect the organization's computer networks, systems and the associated data and information. This includes defining security policies, processes and standards and ensuring established technical controls are configured and maintained. Reports to the Director of Information Technology.

ESSENTIAL FUNCTIONS/TYPICAL TASKS:

(These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position if the work is similar, related, or a logical assignment to the position.)

- Performs highly complex analysis and technical tasks involving assignment and coordination of measures to provide information assurance, event detection and rapid response across various environments of the enterprise;
- Designs, implements and supports integration of information security solutions including Intrusion Prevention systems, firewalls, Intrusion Detective systems, Authentication systems and Security Incident & Event Management systems and developing and coordinating security implementation plans;
- Identifies process functions, risk security weaknesses and controls; presents security challenges and resolutions to management, and implements plans, researches and deploys new technologies, manages transition to operational service;
- Provides technical lead on security projects which involve a wide range of issues including secure architectures, secure electronic data traffic, network security, platform and data security and privacy;
- Provides organizational support of enterprise security architecture and design, benchmarking, technical framework and gap analysis;
- Provides organizational support for developing and implementing security of electronic information during transit and on multi-platform operating systems;
- Reviews and contributes to the security activities portions of Business Application Development Project Plans;
- Works with senior management to determine acceptable levels of risk for enterprise computing platforms and to discuss security implications of new information technology uses being considered;
- Reviews and contributes to the improvement and standardization of the security administration process across all business units;
- Guides users and technical team members in formulating security requirements, integrating security requirements into existing system architectures, developing security test plans, overseeing the execution of security testing, and advising alternative approaches;
- Interacts with other departments and vendors to gather data, resolve and document complex technical issues for implementation of security products;
- Researches and assesses new threats and security alerts, and recommends remedial action;
- Investigates, documents and reports any actual or potential information security violation or inappropriate computers use;
- Leads security management services, forensic analysis, cyber-crime investigation, incident emergency response and investigations;
- Develops and periodically tests strategies and solutions for cybersecurity, privacy, risk, compliance, service continuity, and disaster recovery;
- Prepares training plans for staff, allocates ongoing training for personnel on new computer systems or technologies being implemented which require security administration.
- Performs related tasks as required.

KNOWLEDGE, SKILLS AND ABILITIES:

Comprehensive knowledge of modern methods, concepts, practices, and principles related to information system security. Knowledge of cyber security standards. Audit, compliance or governance experience is preferred. Knowledge of network infrastructure, including routers, switches, firewalls, and the associated network protocols and concepts. Knowledge of enterprise systems and a variety of software applications. Thorough knowledge of research and risk analysis methods and techniques; thorough knowledge of statistical analysis and forecasting techniques. Thorough knowledge of the principles, practices, and techniques of information management technologies; ability to identify, analyze and resolve security incidents; ability to effectively organize, schedule and plan work assignments; ability to plan, schedule, and coordinate special project assignments; ability to translate technical terminology into terms understood by management and employees; ability to establish and maintain effective working relationships with County employees, vendors and the general public; ability to communicate effectively both orally and in writing; ability to establish and maintain effective working relationships with associates and the general public.

EDUCATION AND EXPERIENCE:

Possession of a bachelor's degree in computer science, telecommunications management or Cybersecurity; plus six years of information security systems experience.

PHYSICAL REQUIREMENTS:

This is sedentary work requiring the exertion of up to 10 pounds of force occasionally and a negligible amount of force frequently or constantly to move objects; work requires fingering, grasping and repetitive motions; vocal communication is required for expressing or exchanging ideas by means of the spoken word; hearing is required to perceive information at normal spoken word levels, and to receive detailed information through oral communications and/or to make fine distinctions in sound; visual acuity is required for depth perception, color perception, preparing and

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential tasks.

analyzing written or computer data, determining the accuracy and thoroughness of work, and observing general surroundings and activities; the worker is not subject to adverse environmental conditions.

SPECIAL REQUIREMENTS:
Possession of an appropriate driver’s license valid in the Commonwealth of Virginia. Must pass a criminal background check and credit history check.

Confidentiality Statement

I acknowledge and understand that I may have access to confidential information regarding [employees, students, patients, inmates, and the public]. In addition, I acknowledge and understand that I may have access to proprietary or other confidential business information belonging to Fauquier County. Therefore, except as required by law, I agree that I will not:

- Access data that is unrelated to my job duties at Fauquier County.
- Disclose to any other person, or allow any other person to any information related to Fauquier County that is proprietary or confidential and/or pertains to [employees, students, patients, inmates, the public]. Disclosure of information includes, but is not limited to, verbal discussions, FAX transmissions, electronic mail messages, voice mail communication, written documentation, "loaning" computer access codes, and/or another transmission or sharing of data.

I understand that Fauquier County and its [employees, students, patients, inmates, the public], staff or others may suffer irreparable harm by disclosure of proprietary or confidential information and that Fauquier County may seek legal remedies available to it should such disclosure occur. Further, I understand that violations of this agreement may result in disciplinary action up to, and including, termination of employment.

I have reviewed my job description with my supervisor and understand the duties assigned to me and the measures to which I will be held accountable.

Date____________ Name____

Signature_____________________________________

Date___________ Supervisor____________________________________

Signature_____________________________________

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential tasks.